SÉCURITÉ

Protéger votre messagerie

Ne cliquez jamais

Sur un lien ou une pièce jointe douteuse. Survolez les liens pour vérifier l'URL réelle avant de cliquer.

Ne répondez jamais

À un mail suspect. En cas de doute, contactez l'expéditeur via un autre canal de communication.

Méfiez-vous des QR codes

Reçus par mail sans contexte. Rendez-vous directement sur le site officiel plutôt que de scanner le code.

Changez votre mot de passe

Immédiatement si vous suspectez une compromission, via les outils de réinitialisation de votre académie.

SÉCURITÉ

Reconnaître un mail frauduleux

Que faire si vous recevez un mail suspect ?

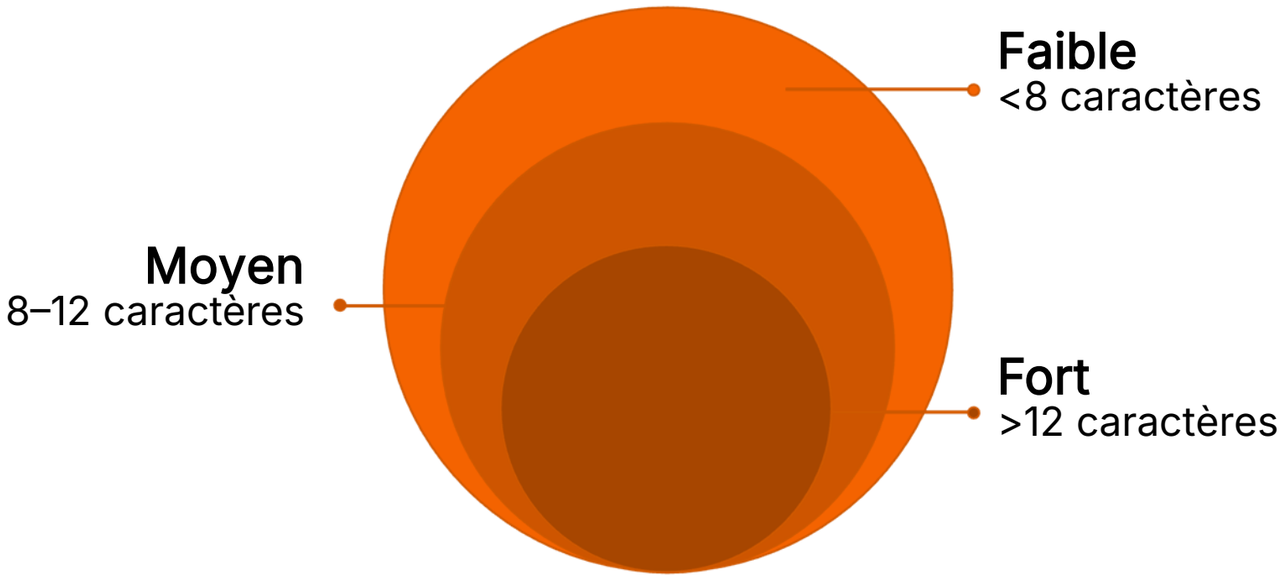
1. **Ne pas répondre ni cliquer**
   Aucun lien, aucune pièce jointe.

2. **Signaler comme spam**
   Utilisez la fonctionnalité dans Zimbra.

3. **Alerter vos collègues**
   Si le mail est confirmé frauduleux.

SÉCURITÉ

Créer un mot de passe robuste



- Minimum **12 caractères** — idéalement plus.
- Combinez **majuscules, minuscules, chiffres et caractères spéciaux**.
- Évitez les informations personnelles (nom, date de naissance...).
- Changez votre mot de passe **tous les 6 mois**.
- Ne l'enregistrez pas dans votre navigateur sur un ordinateur partagé.

⚠ Les pièces jointes chiffrées par mot de passe et certains exécutables (.exe, .bat, .js...) sont automatiquement bloqués par le système.